REDES INALAMBRICAS

Una **red inalámbrica** es, como su nombre lo indica, una red en la que dos o más terminales (por ejemplo, ordenadores portátiles, agendas electrónicas, etc.) se pueden comunicar sin la necesidad de una conexión por cable.
Con las redes inalámbricas, un usuario puede mantenerse conectado cuando se desplaza dentro de una determinada área geográfica. Por esta razón, a veces se utiliza el término "movilidad" cuando se trata este te

INTRODUCCION A LA SEGURIDAD EN REDES INALAMBRICAS

Wired Equivalent Privacy

WEP, acrónimo de ***Wired Equivalent Privacy*** o "Privacidad Equivalente a Cableado", es el sistema de cifrado incluido en el estándar IEEE 802.11 como protocolo para redes Wireless que permite cifrar la información que se transmite. Proporciona un cifrado a nivel 2, basado en el algoritmo de cifrado RC4 que utiliza claves de 64 bits (40 bits más 24 bits del vector de iniciación IV) o de 128 bits (104 bits más 24 bits del IV). Los mensajes de difusión de las redes inalámbricas se transmiten por ondas de radio, lo que los hace más susceptibles, frente a las redes cableadas, de ser captados con relativa facilidad. Presentado en 1999, el sistema WEP fue pensado para proporcionar una confidencialidad comparable a la de una red tradicional cableada.
Comenzando en 2001, varias debilidades serias fueron identificadas por analistas criptográficos. Como consecuencia, hoy en día una protección WEP puede ser violada con software fácilmente accesible en pocos minutos. Unos meses más tarde el IEEE creó la nueva corrección de seguridad 802.11i para neutralizar los problemas. Hacia 2003, la Alianza Wi-Fi anunció que WEP había sido reemplazado por Wi-Fi Protected Access (WPA). Finalmente en 2004, con la ratificación del estándar completo 802.11i (conocido como WPA2), el IEEE declaró que tanto WEP-40 como WEP-104 fueron revocados por presentar fallos en su propósito de ofrecer seguridad. A pesar de sus debilidades, WEP sigue siendo utilizado, ya que es a menudo la primera opción de seguridad que se presenta a los usuarios por las herramientas de configuración de los routers aún cuando sólo proporciona un nivel de seguridad que puede disuadir del uso sin autorización de una red privada, pero sin proporcionar verdadera protección. Fue desaprobado como un mecanismo de privacidad inalámbrico en 2004, pero todavía está documentado en el estándar actual.
WEP es a veces interpretado erróneamente como Wireless Encryption Protocol.

Wi-Fi Protected Access

Wi-Fi Protected Access, llamado también ***WPA*** (en español «Acceso Wi-Fi protegido») es un sistema para proteger las redes inalámbricas (Wi-Fi); creado para corregir las deficiencias del sistema previo, Wired Equivalent Privacy (WEP). Los investigadores han encontrado varias debilidades en el algoritmo WEP (tales como la reutilización del vector de inicialización (IV), del cual se derivan ataques estadísticos que permiten recuperar la clave WEP, entre otros). WPA implementa la mayoría del estándar IEEE 802.11i, y fue creado como una medida intermedia para ocupar el lugar de WEP mientras 802.11i era finalizado. WPA fue creado por The Wi-Fi Alliance («La alianza Wi-Fi»).
WPA adopta la autenticación de usuarios mediante el uso de un servidor, donde se almacenan las credenciales y contraseñas de los usuarios de la red. Para no obligar al uso de tal servidor para el despliegue de redes, WPA permite la autenticación mediante una clave precompartida, que de un modo similar al WEP, requiere introducir la misma clave en todos los equipos de la red.
Una falla encontrada en la característica agregada al Wi-Fi llamada **Wi-Fi Protected Setup** (también bajo el nombre de **QSS**) permite eludir la seguridad e infiltrarse en las redes que usan los protocolos WPA y WPA2.

Historia

WPA fue diseñado para utilizar un servidor de autenticación (normalmente un servidor RADIUS), que distribuye claves diferentes a cada usuario (a través del protocolo 802.1x); sin embargo, también se puede utilizar en un modo menos seguro de clave precompartida para usuarios de casa o pequeña oficina. La información es cifrada utilizando el algoritmo RC4 (debido a que WPA no elimina el proceso de cifrado WEP, sólo lo fortalece), con una clave de 128 bits y un vector de inicialización de 48 bits.
Una de las mejoras sobre WEP, es la implementación del Protocolo de Integridad de Clave Temporal (TKIP - *Temporal Key Integrity Protocol*), que cambia claves dinámicamente a medida que el sistema es utilizado. Cuando esto se combina con un vector de inicialización (IV) mucho más grande, evita los ataques de recuperación de clave (ataques estadísticos) a los que es susceptible WEP.
Adicionalmente a la autenticación y cifrado, WPA también mejora la integridad de la información cifrada. La comprobación de redundancia cíclica (CRC - *Cyclic Redundancy Check*) utilizado en WEP es inseguro, ya que es posible alterar la información y actualizar la CRC del mensaje sin conocer la clave WEP. WPA implementa un código de integridad del mensaje (MIC - *Message Integrity Code*), también conocido como "Michael". Además, WPA incluye protección contra ataques de "repetición" (replay attacks), ya que incluye un contador de tramas.
Al incrementar el tamaño de las claves, el número de llaves en uso, y al agregar un sistema de verificación de mensajes, WPA hace que la entrada no autorizada a redes inalámbricas sea mucho más difícil. El algoritmo Michael fue el más fuerte que los diseñadores de WPA pudieron crear, bajo la premisa de que debía funcionar en las tarjetas de red inalámbricas más viejas; sin embargo es susceptible a ataques. Para limitar este riesgo, los drivers de las estaciones se desconectarán un tiempo definido por el fabricante, si reciben dos colisiones Michael en menos de 60 segundos, podrán tomar medidas, como por ejemplo reenviar las claves o dejar de responder durante un tiempo específico.

Seguridad, ataques WPA TKIP

TKIP es vulnerable a un ataque de recuperación de keystream, esto es, sería posible reinyectar tráfico en una red que utilizara WPA TKIP. Esto es posible por diversas causas, algunas de ellas heredadas de WEP. Entre las causas, cabe destacar la evasión de las medidas anti reinyección de TKIP y se sigue una metodología similar a la utilizada en el popular ataque CHOP CHOP sobre el protocolo WEP. La evasión de protección anti reinyección de TKIP es posible debido a los diversos canales que se utilizan en el modo QoS especificado en el estándar 802.11ie, aunque también existe la posibilidad de aplicarlo en redes no QoS.

WPA2

Una vez finalizado el nuevo estándar 802.11ie se crea el WPA2 basado en este. WPA se podría considerar de «migración», mientras que WPA2 es la versión certificada del estándar de la IEEE.

El estándar 802.11i fue ratificado en junio de 2004.

La alianza Wi-Fi llama a la versión de clave pre-compartida WPA-Personal y WPA2-Personal y a la versión con autenticación 802.1x/EAP como WPA-Enterprise y WPA2-Enterprise.

Los fabricantes comenzaron a producir la nueva generación de puntos de acceso apoyados en el protocolo WPA2 que utiliza el algoritmo de cifrado AES (Advanced Encryption Standard). Con este algoritmo será posible cumplir con los requerimientos de seguridad del gobierno de USA - FIPS140-2. "WPA2 está idealmente pensado para empresas tanto del sector privado cómo del público. Los productos que son certificados para WPA2 le dan a los gerentes de TI la seguridad de que la tecnología cumple con estándares de interoperatividad" declaró Frank Hazlik Managing Director de la Wi-Fi Alliance. Si bien parte de las organizaciones estaban aguardando esta nueva generación de productos basados en AES es importante resaltar que los productos certificados para WPA siguen siendo seguros de acuerdo a lo establecido en el estándar 802.11i

Seguridad ataques WPA2

Tanto la versión 1 de WPA, como la denominada versión 2, se basan en la transmisión de las autenticaciones soportadas en el elemento de información correspondiente. En el caso de WPA 1, en el tag propietario de Microsoft, y en el caso de WPA2 en el tag estándar 802.11i RSN.

Durante el intercambio de información en el proceso de conexión RSN, si el cliente no soporta las autenticaciones que especifica el AP (access point, punto de acceso), será desconectado pudiendo sufrir de esta manera un ataque DoS específico a WPA.

Además, también existe la posibilidad de capturar el 4-way handshake que se intercambia durante el proceso de autenticación en una red con seguridad robusta. Las claves PSK (precompartidas) son vulnerables a ataques de diccionario (no así las empresariales, ya que

el servidor RADIUS generará de manera aleatoria dichas claves), existen proyectos libres que utilizanGPU con lenguajes específicos como CUDA (NVIDIA) y Stream (AMD) para realizar ataques de fuerza bruta hasta cien veces más rápido que con computadoras ordinarias.

Advanced Encryption Standard

Advanced Encryption Standard (**AES**), también conocido como **Rijndael** (pronunciado "Rain Doll" en inglés), es un esquema de cifrado por bloques adoptado como un estándar de cifrado por el gobierno de los Estados Unidos. El AES fue anunciado por el Instituto Nacional de Estándares y Tecnología (NIST) como FIPS PUB 197 de los Estados Unidos (FIPS 197) el 26 de noviembrede 2001 después de un proceso de estandarización que duró 5 años. Se transformó en un estándar efectivo el 26 de mayo de 2002. Desde 2006, el AES es uno de los algoritmos más populares usados en criptografía simétrica.
El cifrado fue desarrollado por dos criptólogos belgas, Joan Daemen y Vincent Rijmen, ambos estudiantes de la *Katholieke Universiteit Leuven*, y enviado al proceso de selección AES bajo el nombre "Rijndael".

CCMP

CCMP es un protocolo de encriptación de IEEE 802.11i. CCMP significa Counter Mode with Cipher Block Chaining Message Authentication Code Protocol.

Fue creado para reemplazar TKIP (el protocolo obligatorio en el WPA), y WEP (un protocolo inseguro).

CCMP es obligatorio en el estándar WPA2, opcional en WPA y obligatorio en las redes RSN (Robust Security Network). CCMP también es usado en el estándar de redes hogareñas y de trabajo ITU-T G.hn.

Características de CCMP

CCMP emplea el algoritmo de seguridad AES (Advanced Encryption Standard). A diferencia de TKIP, la integridad de la clave de administración y mensaje es manejada por un único componente creado alrededor de AES usando una clave de 128 bits, un bloque de 128 bits y 10 rondas de codificación por el estándar FIPS 197.

TKIP

TKIP (***T**emporal **K**ey **I**ntegrity **P**rotocol*) es también llamado hashing de clave WEP WPA, incluye mecanismos del estándar emergente 802.11i para mejorar el cifrado de

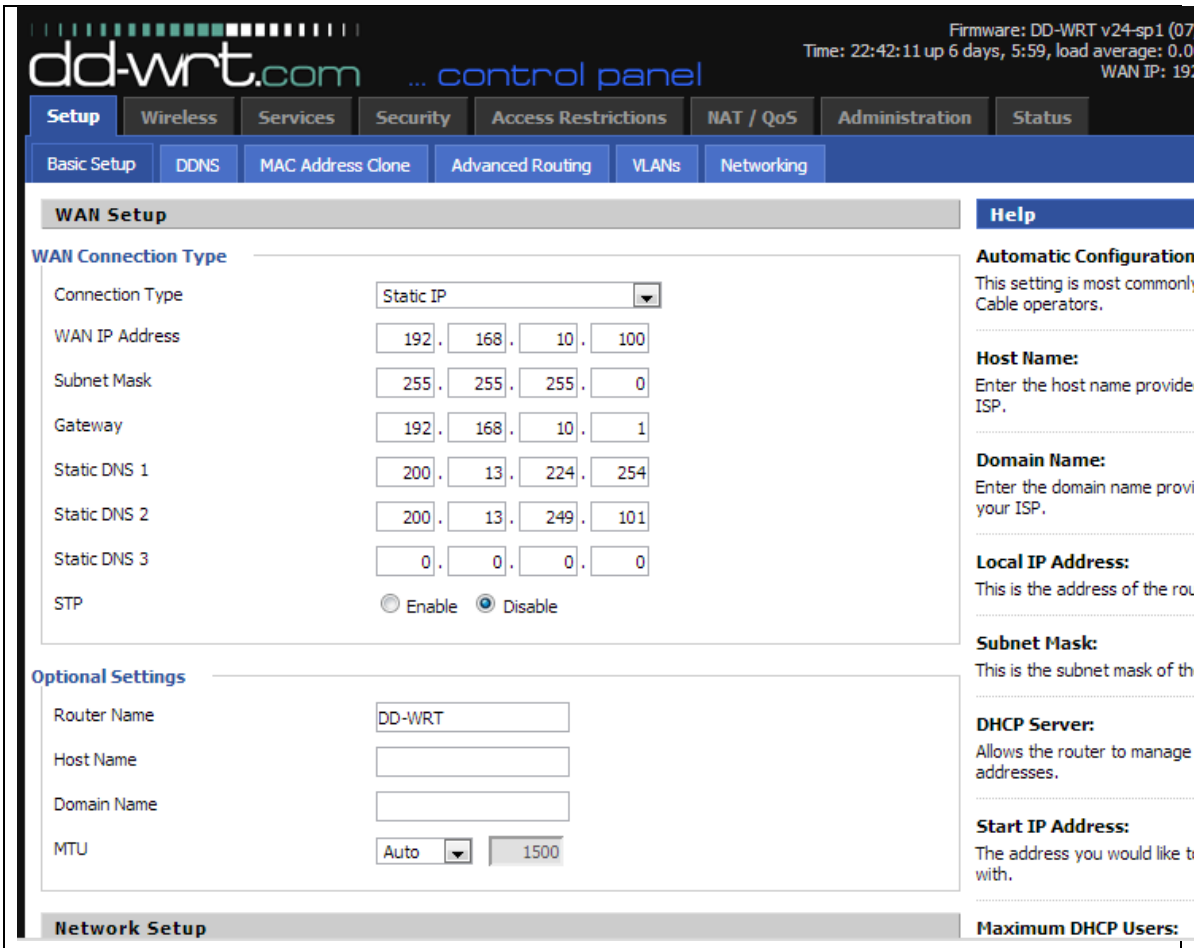
datos inalámbricos. WPA tiene TKIP, que utiliza el mismo algoritmo que WEP, pero construye claves en una forma diferente. Esto era necesario porque la ruptura de WEP había dejado a las redes WiFi sin seguridad en la capa de enlace, y se necesitaba una solución para el hardware ya desplegado.

Si has comprendido los conceptos anteriores los parámetros de configuración serán sencillos de escoger de acuerdo a las necesidades del cliente.

MANUAL DE CONFIGURACION equipo WRT300N de la Marca Linksys

En el momento de configurar los equipos AP, no todos presentan iguales campos de configuración, unos con más características y otros básicos, esto se debe a la variedad de equipos y marcas. La mayoría de ellos dan opciones de cambio de sistema operativo o más conocido como FLASHEO gracias a la web http://www.dd-wrt.com donde puedes encontrar el listado de marcas y modelos soportados con sus respectivos tutoriales para ejecutar el cambio del Sistema Operativo.

En la siguiente imagen observas un equipo WRT300N de la Marca Linksys en la WEB de configuración principal.



Para ingresar al sistema de configuración de un equipo activo, debes conocer la dirección IP y estar seguro que el servicio web este activo. Luego de conocer su dirección IP que generalmente es la puerta de enlace, ingresamos a nuestro explorador de internet e ingresamos en el campo de direcciones la dirección IP del equipo activo (generalmente el puerto por defecto es el puerto 80, pero puede ocurrir que algunos modelos o aun luego de haberse configurado se haya cambiado por otro puerto como el 8080).

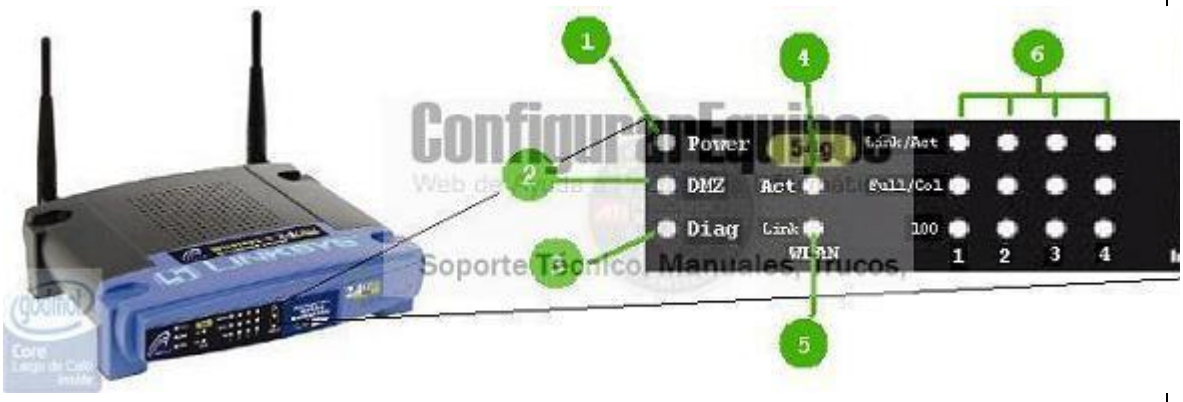
En este momento aparecen campos de autenticación, y para ellos debemos ingresar con el usuario y contraseña, si es un equipo nuevo, debes revisar el manual de instalación y configuración para encontrar los valores por defecto, de lo contrario, debes consultar con el administrador de la red, o si tu equipo lo has adquirido de segunda mano, debes reiniciar tales configuraciones a configuraciones de fábrica (busca en el manual técnico del equipo como ejecutar procedimiento de reinicio a valores por defecto haciendo uso del botón reset).

A continuación encuentras un tutorial paso a paso para configurar un equipos WRT54G de Linksys.

En este tutorial vamos a tratar de explicar cómo configurar todo un clásico, el router **Linksys WRT54G**, y ponerlo en marcha de la manera más sencilla posible.

Este router es único entre los dispositivos de consumo doméstico, esto se debe a que los desarrolladores de Linksys tuvieron que liberar el código fuente del firmware del dispositivo para cumplir con las obligaciones de la **GNU GPL** (*General Public License* o licencia pública general) relacionada con la libre distribución de software. Este hecho permite a los entusiastas de la programación modificar el firmware para añadir o cambiar funcionalidades del dispositivo. Actualmente existen varios proyectos de desarrollo que proveen versiones mejoradas del firmware para el WRT54G.

En primer lugar vamos a ver como es el router y sus características básicas, en la imagen que vemos a continuación, podemos observar la parte frontal del router:



Aunque también podría tener este otro aspecto:

En la imagen vemos diferentes LEDS y describimos a continuación los correspondiente a la primera imagen:

1 - LED Power.

En verde, indica que el router está encendido.

2 - LED DMZ.

Nos indica que está habilitada la opción **DMZ** (*DesMilitarized Zone*) en la que hay algún equipo que se encuentra fuera de la zona de seguridad, por la propia configuración del router.

3 - LED Diag.

En rojo durante el arranque, nos indica que el router se encuentra haciendo el autotest y se apagará en cuanto acabe el mismo. Si permanece encendida por más de un minuto es que el autotest ha encontrado algún problema.

4 - LED Act.

Este Led, también de color verde, nos proporciona información del estado de la red inalámbrica. Si el Led está intermitente indica que a través de la red se esta produciendo envío o recepción de datos.

5 - LED Link.

Sí está encendido, indica que la red inalámbrica está habilitada.

6 - LED´s de estado de la red local.

Hay cuatro juegos de leds, uno para cada uno de los puertos de la LAN y su significado es:

- Link/Act es de color verde e indica que hay un dispositivo conectado al puerto. Si está

intermitente nos advierte que la conexión es correcta y se están recibiendo o transmitiendo datos

- Full/Col también es de color verde y nos indica, si está fijo, que la comunicación es *Full Duplex*. Si está intermitente indica que hay colisiones entre los diferentes paquetes que se envían.

- 100 es un LED de color naranja que indica que la comunicación se realiza a *100 Mbps*. Si se encuentra apagado es que la comunicación es a *10Mbps*.

7 - LED´s Internet.

- Link/Act es de color verde e indica que hay una conexión correcta con la línea ADSL. Si está intermitente nos advierte que la conexión es correcta y se están recibiendo o transmitiendo datos

- Full/Col también es de color verde y nos indica, si está fijo, que la comunicación es *Full Duplex*. Si está intermitente indica que hay colisiones entre los diferentes paquetes que se envían.

- 100 es un LED de color naranja que indica que la comunicación a través de ese puerto se realiza a *100Mbps*. Si se encuentra apagado es que la comunicación es a *10Mbps*.

Si nos fijamos en la parte de atrás del router como vemos en la siguiente imagen:

Tenemos los siguientes elementos

8 - Antenas para comunicación inalámbrica.

9 - Botón Reset.

Este botón permite restaurar la configuración de fábrica del router.

10 - Puerto ADSL.

11 - Puertos Ethernet.

Estos puertos nos van a permitir conectar dispositivos al router a través de cables RJ45.

12 - Conector para el adaptador de corriente.

Es el conector para la fuente de alimentación. El fabricante recomienda usar únicamente el adaptador que acompaña al router.

Entre las principales características de router podemos destacar las siguientes:

- ✓ Compartir la conexión a Internet a través de cable o red inalámbrica.
- ✓ Red inalámbrica 802.11g de alta velocidad, compatible con ordenadores Windows, Mac o Linux.
- ✓ Sistema de configuración Web, puede funcionar como servidor virtual para acceso remoto Web, FTP y otros servicios de red.

2.- Cómo conectar el router:

En primer lugar, revisaremos si están todos los elementos que son necesarios para que funcione el Router, esto es, el propio aparato, el adaptador de corriente para proporcionarle alimentación, un cable par trenzado (ocho hilos) con conectores RJ45 que nos permitirá conectar el Router con el dispositivo de conexión a la línea ADSL.

A diferencia de los routers descritos hasta el momento, este modelo de router no es capaz de conectar directamente a la linea ADSL, sino que más bien está preparado para proporcionar conectividad entre un **Cablemodem** o un router que no sea inalámbrico y el resto de la red.

Para ver como quedaría, mostramos la siguiente imagen:

Vamos a ver dos formas de conexión, la primera conectando con un MODEM de banda ancha, y la segunda con conexión con otro router que es el que proporciona la conectividad ADSL.

Instalación del hardware para la conexión al módem de banda ancha.

En primer lugar, para realizar las conexiones y evitar riesgos innecesario tanto para nosotros como para los equipos vamos a tomar la precaución de desconectar la alimentación eléctrica de los equipos.
A continuación hay que buscar el lugar mas adecuado para el router ya que, para aprovechar al máximo su capacidad inalámbrica, debería situarse en el centro de la red inalámbrica así todos los equipos puedan tener fácil acceso a él.

Vamos a realizar las conexiones con el resto de quipos, para ello conectamos un cable de red Ethernet estándar RJ45 al puerto Internet del router como vemos en la imagen:

Conectamos el otro extremo del cable Ethernet al módem de banda ancha por cable o DSL. A continuación vamos conectando los PC que tengan adaptadores de red ethernet y sea necesario usar los puertos RJ45 del router.

Podremos conectar hasta cuatro equipos mediante este tipo de conexión. Una vez conectador los equipos vamos a conectar el cable de alimentación del router.

Así tenemos el router listo para iniciar su configuración acción que vamos a ver más adelante.

Instalación del hardware para la conexión a otro router.

La otra forma de conectar este router es a través de la conexión con otro router. Para evitar conflictos de IP lo primero que vamos a hacer es entrar en la configuración del otro router y

modificar su dirección IP en nuestra red local. Normalmente la dirección que tenga el router será **192.168.1.1** y se la vamos a cambiar por**192.168.2.1**. Eso nos permitirá asignar al **WRT54G** la IP **192.168.1.1** cuando lo configuremos.

Como hemos visto en el caso anterior, debemos desconectar los equipos de sus correspondientes sistemas de alimentación y buscar la ubicación más adecuada para el router para que la cobertura inalámbrica sea la más adecuada para todas las estaciones inalámbricas.

El esquema de conexión podemos verlo en la siguiente imagen:

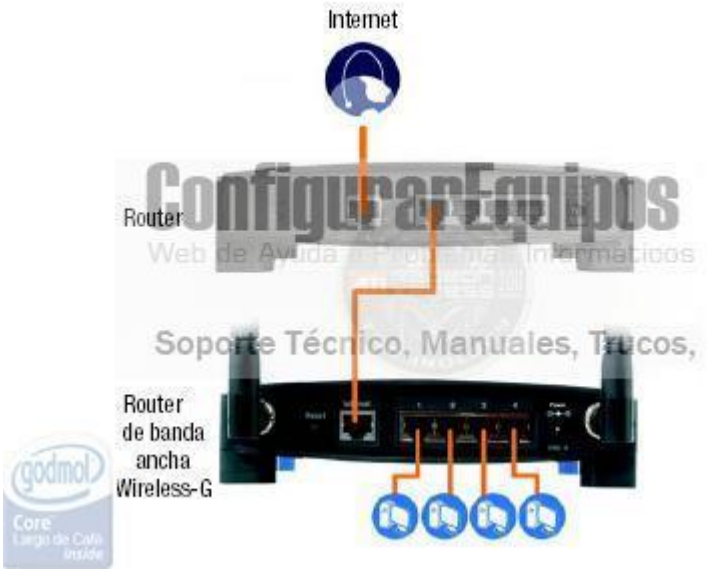


Imagen08

Para mayor claridad se pueden observar las imágenes 05, 06 y 07 en las que se puede apreciar como y dónde se conectará el otro router, los equipos de la red y el adaptador de corriente.

Dejamos el router preparado para iniciar su configuración.

3.- Formas de configurar el router y acceso a la configuración:

Hay dos formas de configurar el equipo. La primera a través del programa que proporciona el propio fabricante en un CD-Rom mediante el asistente de configuración, esta forma es recomendable usarla si no se tiene muy claro lo que hay que poner o si es la primera configuración. La segunda forma es accediendo directamente al programa de configuración que posee por defecto el router y al que se accede a través de cualquier navegador.

En este tutorial trataremos de describir las páginas del configurador Web que incorpora el propio router y las funciones de cada una de esas páginas

Para entrar en el programa de configuración basta con teclear en la barra de direcciones de Internet Explorer la dirección IP del router. Debemos tener en cuenta que la dirección será **192.168.0.1** si el router es nuevo o si no se ha modificado esta dirección en una configuración anterior. Si hemos modificado la dirección IP habrá que teclear la que corresponda.

Aparece una página en la que se solicita una contraseña, debemos dejar el campo Nombre de usuario en blanco.

Imagen09

Es importante tratar de realizar la configuración del router mediante conexión con cable. En muchos casos la red inalámbrica viene desactivada por defecto, y si vamos a cambiar algún parámetro relacionado con la configuración inalámbrica podemos perder la conexión con el router a través de la tarjeta inalámbrica.

Debemos introducir los valores de usuario y palabra clave para acceder a la configuración, los valores de fábrica son

Usuario: se dejarán en blanco, es decir no se introduce nada.
Password: admin

La primera página que aparece si el usuario y la clave son correctos es la que podemos ver en la siguiente imagen:

Imagen10

La primera pantalla que aparece muestra la ficha **Setup** (Configuración). Permite cambiar los parámetros
generales del router.

4.- Configuración básica:

Como hemos visto en el apartado anterior, al entrar en la configuración del router nos aparece la pantalla de la configuración básica del router.

En la sección **Internet Setup** (Configuración de Internet) se configura el router para la conexión a Internet, teniendo en cuenta que la mayor parte de la información a introducir la puede proporcionar nuestro proveedor de conexión.

- Internet Connection Type (Tipo de conexión a Internet)
Hay que elegir en el menú desplegable el tipo de conexión a Internet que proporcione nuestro proveedor. Por defecto, la opción que viene configurada es **Configuration -**
DHCP (Configuración automática - DHCP). en este tipo de conexión a Internet (Internet

Connection Type) el router está configurado en automático y sólo se debe conservar si el proveedor admite DHCP o si se realiza la conexión mediante una dirección IP dinámica.

Las otras opciones son:

Static IP (IP estática). Al seleccionar esta opción se nos presentarán para rellenar los parámetros que vemos en la siguiente imagen:

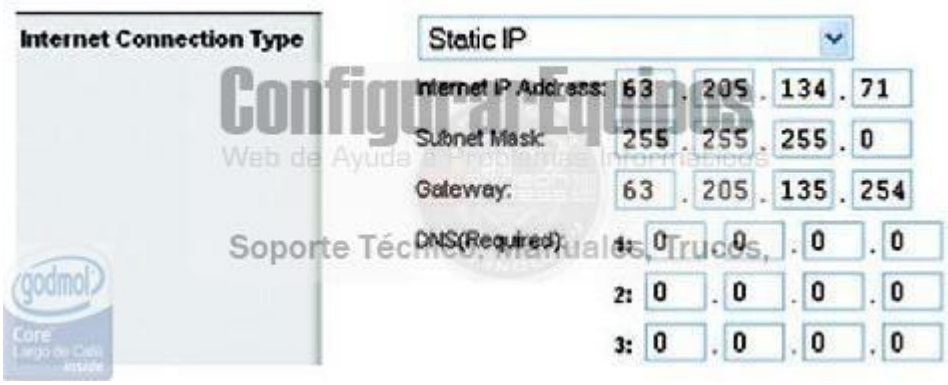

Internet Connection Type
Static IP
Internet IP Address: 63 . 205 . 134 . 71
Subnet Mask: 255 . 255 . 255 . 0
Gateway: 63 . 205 . 135 . 254
DNS(Required) 1: 0 . 0 . 0 . 0
2: 0 . 0 . 0 . 0
3: 0 . 0 . 0 . 0

Imagen11

Si se desea o se necesita utilizar una dirección IP permanente para conectarse a Internet, normalmente este servicio hay que solicitarlo y pagarlo aparte. En este caso, en el campo **Internet IP Address** (Dirección IP de Internet) se introducirá la dirección IP del router, vista desde Internet. El proveedor proporcionará la dirección IP que se debe especificar aquí.

También proporcionará la máscara de subred correspondiente al valor del campo **Subnet Mask**, la **Puerta de enlace** o *Gateway* y al menos una dirección **IP de servidor DNS** (sistema de nombres de dominio).

PPPoE. Al seleccionar esta opción se nos presentarán para rellenar los parámetros que vemos en la siguiente imagen:

Imagen12

Algunos proveedores de ADSL utilizan **PPPoE** (*protocolo de punto a punto en Ethernet*) para establecer conexiones a Internet. Si conectamos a Internet a través de este método hay que consultar con el proveedor los valores de los parámetros siguientes:
- User Name (Nombre de usuario).
- Password (Contraseña).
En los dos campos debemos introducir los valores que nos indique el proveedor.
El parámetro **Connect on Demand: Max Idle Time** (Conectar cuando se solicite: Tiempo máximo de inactividad) nos permitirá configurar el router para que interrumpa la conexión a Internet cuando esté inactiva durante un periodo de tiempo especificado (Max Idle Time, Tiempo máximo de inactividad). Si la conexión a Internet finaliza debido a la inactividad, esta opción de Conectar cuando se solicite permite al router restablecer la conexión automáticamente si intenta acceder de nuevo a Internet.

Para activar **Connect on Demand** (Conectar cuando se solicite), sólo hay que seleccionar el *radio Button* y en el campo **Max Idle Time** (Tiempo máximo de inactividad), introducir el número de minutos de inactividad que desea que transcurran antes de finalizar la conexión a Internet.

Si no deseamos que la conexión se interrumpa, debemos seleccionar en el *Radio Button* **Keep Alive: Redial Period** (Mantener activo: Periodo para nueva marcación). Si tenemos seleccionada esta opción, el router comprobará periódicamente la conexión a Internet y si se desconecta, el router restablecerá automáticamente la conexión. El campo **Redial Period** (Periodo para nueva marcación) especificara la frecuencia con que desea que el router compruebe la conexión a Internet. El valor predeterminado para la nueva marcación es de 30 segundos.

Disponemos también de un conjunto de Parámetros opcionales **Optional Settings** que podemos ver en la siguiente imagen:

Imagen13

Es posible que nuestro proveedor de conexión necesite estos parámetros y son:

Router Name (Nombre de router). En donde escribiremos un nombre de hasta 39 caracteres para identificar el router.

Host Name/Domain Name (Nombre de host/Nombre de dominio). En estos campos puede proporcionar un nombre de host y de dominio para el router que algunos proveedores de conexión, normalmente los de cable, solicitan como identificación. Como es lógico habrá que consultar con el Proveedor de conexión si el servicio de Internet de banda ancha se ha configurado con un nombre de host y de dominio. Normalmente no habrá ningún problema si se dejan estos campos en blanco.

MTU. Corresponde a la unidad de transmisión máxima. Especifica el tamaño máximo de paquete permitido para la transmisión de Internet. Por defecto el valor que viene seleccionado es **Manual**, y permite introducir el tamaño máximo de paquete que se transmitirá. El tamaño recomendado, que se introduce en el campo **Size**(Tamaño), es **1492**. Este valor debe estar en el intervalo de **1200** a **1500**. Para que el router seleccione la**MTU** óptima para la conexión a Internet, seleccionaremos **Auto** (Automática).

Dentro de la configuración básica nos queda por ver la parte de configuración de la red local, y ésto se realizará en la parte de la pantalla correspondiente a los parámetros **Network Setup** (Configuración de red) que nos permite cambiar los parámetros de la red local a la que está conectado el router.

El primer parámetro a configurar es **Router IP** (IP del router), como vemos en la imagen que aparece a continuación:

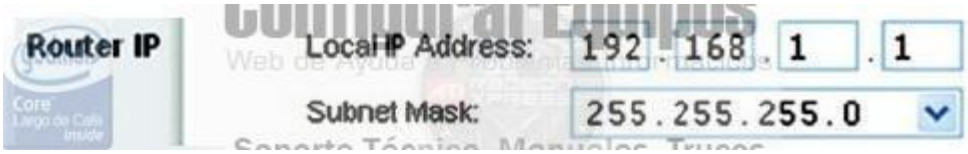


Imagen14

Este parámetro nos permitie configurar la *dirección IP del router* (IP Address) y la *máscara de subred* (Subnet Mask) del router tal como las ve la red interna.

Por último, nos falta por describir los Parámetros de servidor de direcciones de red, *DHCP Network Address Server Settings* (DHCP), como vemos en la imagen

Network Address Server Settings (DHCP)
DHCP Server: Enable Disable
Starting IP Address: 192.168.1. 100
Maximum Number of DHCP Users: 50
Client Lease Time: 0 minutes (0 means one day)
Static DNS 1: 0 . 0 . 0 . 0
Static DNS 2: 0 . 0 . 0 . 0
Static DNS 3: 0 . 0 . 0 . 0
WINS 0 . 0 . 0 . 0

Imagen15

Estos parámetros permiten configurar la función de servidor de protocolo de configuración dinámica de host (DHCP) del router. El router se puede utilizar como servidor DHCP para la red. Un servidor DCHP asigna automáticamente una dirección IP a cada ordenador de la red. Si desea activar la opción de servidor DHCP del router, se deben configurar todos los PC de la red para que se conecten a un servidor DHCP (el router) y asegurarse de que no hay otro servidor DHCP en la red.

Por defecto el DHCP viene activado de fábrica. Si ya tenemos un servidor DHCP en la red o si no queremos utilizar un servidor DHCP, marcaremos el *Radio button* como **Disable**.

Si tenemos activado el servidor DHCP, el valor del parámetro **Starting IP Address** (Dirección IP inicial) indicará la dirección a partir de la que se empezarán a asiganar direcciones IP automáticas a los equipos de la red. Debido a que la dirección IP predeterminada del router es **192.168.1.1**, la dirección IP inicial debe ser**192.168.1.2** o mayor, pero menor que **192.168.1.253**.

La dirección IP inicial predeterminada es **192.168.1.100**. Eso significaría que ningún equipo de la red que solicite IP de forma automática tendría direcciones IP inferiores a **192.168.1.100**. Este tipo de característica nos permitirá asignar las direcciones que el DHCP no va a asignar de manera automática en nuestra red a equipo que deban cumplir alguna función específica y deban tener IP interna fija.

Los parámetros que hemos visto se combinan con **Maximum Number of DHCP Users** (Número máximo de usuarios de DHCP), que indica el número máximo de ordenadores a los que el Servidor DHCP proporcionará un IP de manera automática. Este número no puede superar los **253** y su valor por defecto es **50**.

Por último nos queda el parámetro **Client Lease Time** (Tiempo de concesión del cliente), que corresponde al tiempo máximo que un usuario podrá estar conectado al router con la dirección

IP dinámica actual. Una vez transcurrido este tiempo, al usuario se le asignará automáticamente una nueva dirección IP dinámica. Por defecto, el valor es **0**, lo que indica que es un día.

La últimos valores que aparecen en la pantalla corresponde a las direcciones IP de los servidores DNS, que es el método que se utiliza en Internet para traducir los nombres de dominio o sitio Web a direcciones de Internet o URL. El Proveedor nos indicará al menos uno de estos valores. En la imagen que vemos a continuación se pueden ver los más habituales:

Proveedor	DNS
Arrakis	< 195.5.64.2 > < 195.5.64.6 >
Arsys	< 217.76.128.4 > < 217.76.129.4 >
Auna	< 62.81.31.250 > < 62.81.61.2 >
Comunitel	< 212.145.4.97 > < 212.145.4.98 >
Eresmas	< 62.81.0.33 > < 62.81.16.129 >
Euskaltel	< 212.55.8.132 > < 212.55.8.133 >
Jazztel	< 62.14.63.145 > < 62.14.2.1 >
Jazztel 20Mb	< 87.216.1.65 > < 87.216.1.66 >
Metrored	< 80.251.75.5 > < 80.251.75.6 >
Onetic Tel	< 213.195.64.129 > < 209.195.79.129 >
Telefónica	< 80.58.0.33 > < 80.58.32.97 >
Tele 2	< 130.244.127.161 > < 130.244.127.169 >
Terra	< 194.224.52.36 > < 194.224.52.37 >
Tiscali	< 194.224.52.36 > < 194.224.52.37 >
Wanadoo	< 195.130.224.18 > < 195.130.225.129 >
Ya.com	< 62.37.237.140 > < 62.37.236.252 >
	< 62.151.2.8 > < 62.151.4.21 >

ConfigurarEquipos
Soporte Técnico, Manuales, Trucos,

Imagen16

Además de todos los parámetros de configuración, podemos acceder a otra opción de configuración, que vemos en la imagen:

Imagen17

Este parámetro corresponde a la configuración horaria, que nos permite elegir la zona horaria desde el desplegable correspondiente e incluso seleccionar si queremos que se ajuste

automáticamente para el horario de verano.

5.- Configuración avanzada:

Hemos visto dentro de la pestaña **SetUp** la opción de configuración básica, pero además hay que tener en cuenta el resto de opciones que vamos a ir detallando a continuación.

Pestaña DDNS:

El router proporciona una función de sistema dinámico de nombres de dominio (DDNS). Este servidor DDNS permite asignar un nombre de host y de dominio fijo a una dirección IP dinámica de Internet. Esto es útil si necesitamos alojar nuestro propia página Web, servidor FTP u otro servidor que se encuentre detrás del router. Para poder utilizar esta función debe suscribirse al servicio DDNS con un proveedor de dicho servicio. Si pinchamos en la opción nos aparece la siguiente pantalla:

Imagen18

Los parámetros a introducir en esta pantalla son:

DDNS Service (Servicio DDNS). Se debe seleccionar el servicio DDNS con el que trabaja en el menú desplegable.
User Name (Nombre de usuario). Corresponde al nombre de usuario de la cuenta DDNS.
Password (Contraseña). Es la contraseña de la cuenta DDNS.
Host Name (Nombre de host). Se trata de la URL de DDNS asignada por el servicio DDNS.
Internet IP Address (Dirección IP de Internet). Corresponde a la dirección IP actual del router hacia Internet.
Status (Estado). Muestra el estado de la conexión DDNS.

Una vez introducidos los valores se debe hacer clic en el botón **Save Settings** para aplicar los cambios o en**Cancel Changes** para cancelarlos.

Pestaña MAC Address Clone (Clonación de direcciones MAC).

Recordaremos que una dirección MAC es un código de 12 dígitos asignado a un dispositivo de hardware para su identificación (tarjeta de red conectada a un PC). Algunos proveedores de conexión requieren que se registre una dirección MAC para acceder a Internet. Si no queremos volver a registrar de nuevo la dirección MAC con nuestro proveedor, se puede asignar al router la dirección MAC que tengamos registrada actualmente con él mediante la función de clonación de direcciones MAC.

Si pinchamos en la opción nos aparece la siguiente pantalla:

Imagen19

Los parámetros a introducir en esta pantalla son:

Enable/Disable (Activar/Desactivar). Para activar/desactivar la clonación de dirección MAC seleccionamos los *radio buttons* **Activas/desactivar**.

User Defined Entry (Entrada definida por el usuario). Nos permite insertar la dirección MAC registrada con el proveedor.

Clone Your PCs MAC Address (Clonar la dirección MAC del PC). Este botón nos permite habilitar la clonación de la dirección MAC.

Una vez introducidos los valores se debe hacer clic en el botón **Save Settings** para aplicar los cambios o en**Cancel Changes** para cancelarlos.

Pestaña Advanced Routing.

Esta opción de configuración se utiliza para configurar las funciones avanzadas del router. Además debemos tener en cuenta que dependiendo del modo de funcionamiento elegido la pantalla va a variar.

Si elegimos en el menú desplegable la forma de funcionamiento **Gateway** (Puerta de enlace) se nos presentará un pantalla como la que vemos en la imagen:

Imagen20

Seleccionaremos este modo de funcionamiento si el router aloja la conexión a Internet de la red.

Por el contrario, si existe otro router en la red seleccionaremos el modo de funcionamiento **Routing**, como podemos ver en la imagen siguiente:

Imagen21

Al seleccionar este modo de funcionamiento, se activará la opción **Dynamic**

Routing (Enrutamiento
dinámico) y podremos habilitarla desplegando el menú.

Esta función permite que el router se ajuste automáticamente a los cambios físicos que se produzcan en el diseño de la red e intercambie tablas de enrutamiento con los demás routers. El router determina la ruta de los paquetes de red según el menor número de saltos entre el origen y el destino. El valor predeterminado de esta función es **Disabled** (Desactivado).

Tenemos otro menú desplegable también en el que podemos seleccionar varias opciones:

puede seleccionar **LAN & Wireless** (Red LAN e inalámbrica), que realiza un enrutamiento dinámico por las redes Ethernet e inalámbrica.

También puede seleccionar **WAN**, que realiza un enrutamiento dinámico con los datos procedentes de Internet.

Finalmente, al seleccionar **Both** (Ambas) se permite el enrutamiento dinámico para ambas redes, así como para los datos procedentes de Internet.

Tenemos también posibilidad de definir funciones de **Static Routing** (Enrutamiento estático). Una ruta estática es la ruta predeterminada por la que se desplaza la información de red hasta alcanzar un host determinado o una red concreta.

Para configurar una ruta estática entre el router y otra red, seleccionamos un número en la lista desplegable**Static Routing** (Enrutamiento estático). Una vez elegido el número en la lista hay que introducir la siguiente información:

Delete This Entry (Eliminar esta entrada) para eliminar una ruta estática seleccionada.

Enter Route Name (Introducir nombre de ruta). Introduzca aquí el nombre de la ruta para identificarla, con un máximo de 25 caracteres alfanuméricos.

Destination LAN IP (IP de red LAN de destino). Es la dirección de la red o el host remoto al que desea asignar una ruta estática.

Subnet Mask (Máscara de subred). La máscara de subred determina qué parte de una dirección IP de red LAN de destino corresponde a la parte de la red y cuál a la parte del host.

Default Gateway (Puerta de enlace predeterminada). Se trata de la dirección IP del dispositivo de puerta de enlace que permite el contacto entre el router y la red o el host remoto.

Interface (Interfaz). Esta interfaz indica si la dirección IP de destino se encuentra en *LAN & Wireless* (redes Ethernet e inalámbricas), *WAN* (Internet) o *Loopback* (Retorno de bucle; una red ficticia en la que un PC actúa de red y que es necesaria para determinados programas).

El botón **Show Routing Table** (Mostrar tabla de enrutamiento) nos permite ver las rutas estáticas que ya se han configurado.

Una vez introducidos los valores se debe hacer clic en el botón **Save Settings** para aplicar los cambios o en**Cancel Changes** para cancelarlos.

6.- Configurar red inalámbrica y Filtrado por dirección MAC:

hemos visto de manera general como configurar los datos del router y ahora vamos a ver de manera detallada como se configura la red inalámbrica.
Si pinchamos en la pestaña **Wireless** del menú se nos presenta una pantalla como la que vemos a continuación:

Imagen22

Vemos que hay varias pestañas para configurar y la que nos aparece activada es **Basic Wireless Settings**donde debemos introducir los parámetros básicos para configurar la red inalámbrica. Estos parámetros son:

Wireless Network Mode (Modo de red inalámbrica). Es un menú desplegable en el que podemos elegir los estándares inalámbricos admitidos en la red: Estos son **802.11g** y **802.11b**. Conviene mantener el parámetro predeterminado **Mixed** (Mixto) si no lo tenemos claro o queremos que cualquier dispositivo pueda conectarse.

Seleccionaremos **Disable** para desactivar la red inalámbrica.

Wireless Network Name (SSID). EL SSID (el valor de este parámetro) debe ser un nombre único

que identifique nuestra red inalámbrica de tal forma que todos los equipos que quieran conectarse a ella usen el mismo SSID. Se debe introducir un nombre descriptivo de hasta 32 caracteres tratando de evitar nombres como *default*, *wireless* y/o cualquier otro identificador que no nos resulte suficientemente descriptivo (se puede utilizar cualquier carácter del teclado).

Wireless Channel (Canal inalámbrico) nos permite elegir el canal de transmisión adecuado para la transmisión.

Wireless SSID Broadcast (Difusión inalámbrica de SSID). Este parámetro es muy importante en la configuración de la red inalámbrica a nivel de seguridad y normalmente no le hacemos caso. Si se establece el valor **DISABLE**, se impide que cualquier equipo en el radio de acción de nuestra red inalámbrica detecte el SSID de nuestra red al realizar una operación como la de Ver redes inalámbricas disponibles. De esta manera añadimos un elemento de seguridad adicional al resto de mecanismos de seguridad que tengamos habilitados, ya que a primera vista no se verá la red, limitando los intentos de acceso no deseados. Si seleccionamos el valor **ENABLE** cualquier equipo que solicite una operación para ver las redes inalámbricas disponibles verá el SSID y podrá intentar acceder. Que lo consiga o no ya es otra cosa.

Una vez introducidos los valores se debe hacer clic en el botón **Save Settings** para aplicar los cambios o en**Cancel Changes** para cancelarlos.

Si pulsamos sobre la segunda opción, **Wireless Security** (Seguridad inalámbrica), nos aparecerá una pantalla como la que vemos a continuación:

Imagen23

Los parámetros de la ficha **Wireless Security** (Seguridad inalámbrica) nos permitirán configurar la seguridad de la red inalámbrica. El router admite cuatro opciones de modo de seguridad inalámbrica a elegir desde el menú desplegable:

- WPA Personal.
- WPA Enterprise.
- WPA2 Personal.
- WPA2 Enterprise.
- RADIUS.
- WEP.

Dependiendo del método de seguridad elegido, se nos presentará la pantalla correspondiente inicialmente el sistema de seguridad a utilizar en la red inalámbrica debe ser seguridad **WPA** (*WiFi Protected Access*) Personal, el sistema WPA proporciona cambios de clave dinámicos y es la mejor solución de seguridad, aunque debemos tener en cuenta que en redes en las que no todos los dispositivos soporten WPA será necesario usar**WEP** (*Wired Equivalent Privacy*).

Imagen24

En la pantalla debemos rellenar el campo **WPA Shared Key**. Este campo es una contraseña con un formato de palabra, frase o serie de números y letras que debe tener una longitud entre 8 y 63 caracteres y puede incluir espacios y símbolos especiales. Es necesario que cada cliente que se conecte a la red use la misma contraseña.
El parámetro **GroupKey Retrieval** es el tiempo que tarda en renovarse la clave.

WEP (*Wired Equivalent Privacy*) es el mecanismo básico para transmitir datos de manera segura a través de la red inalámbrica. Las claves de encriptación deben configurarse en el router y después en los equipos clientes que se conecten a la red. Si seleccionamos este método nos aparecerá la siguiente pantalla:

Imagen25

si elegimos **128-bit WEP** para configurar las clave, se deben introducir bien 13 pares de dígitos hexadecimales (0-9, A-F), o bien un valor en el campo **Passphrase** y pulsar en el botón **Generate** para generar los dígitos hexadecimales correspondiente a la clave.

si elegimos **64-bit WEP** como modo de seguridad, para configurar las clave, se deben introducir bien 5 pares de dígitos hexadecimales (0-9, A-F), o bien un valor en el campo **Passphrase** y pulsar en el botón **Generate**para generar los dígitos hexadecimales correspondiente a la clave.

Además, para el modo **64-bit WEP** se pueden introducir hasta cuatro claves en los campos Key 1 a Key 4, siendo el *Radio Button* que aparece delante de cada una de las claves el que indica cual es la que se usa en la transmisión.

Si la opción seleccionada es **WPA Enterprise** el funcionamiento es similar a la primera opción **WPA Personal**descrita, pero en este caso aparecerá la siguiente pantalla:

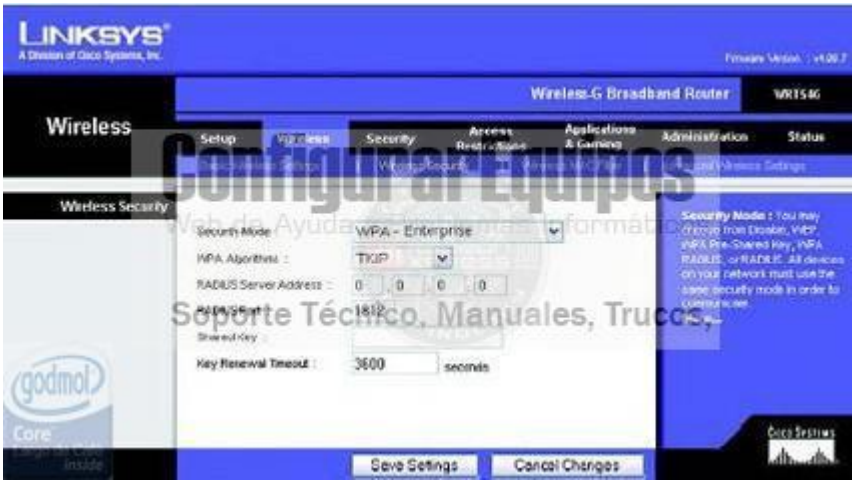


Imagen26

que nos va a permitir configurar la seguridad mediante la gestión de clave por medio de un servidor **Radius**. En este sentido hay que mencionar que para que esto funcione, en la red debe estar ejecutándose un servidor de este tipo. Los parámetros a configurar son la dirección IP del servidor de Radius y que se pondrá en el campo **RADIUS Server Address**. También hay que teclear el puerto por el que trabaja el servidor Radius, y la clave del servidor Radius en el campo **Shared Key**.

Las opciones **WPA2 Personal** y **WPA2 Enterprise** se configurarán de manera parecida a las WPA descritas, aunque hay que mencionar que el nivel de seguridad es mayor.

La tercera pestaña de configuración de la red inalámbrica corresponde a la opción **Wireless MAC Filter** o Filtrado por dirección MAC. Si pulsamos sobre ella se nos presenta la siguiente pantalla:

Imagen27

El funcionamiento de esta pantalla es muy simple. En la parte superior, y mediante la elección de un *Radio Button*, podemos habilitar seleccionando la opción **Enable** o deshabilitar seleccionando la opción **Disable**.

Si hemos habilitado el filtrado, para permitir el acceso a la red inalámbrica de cualquier equipo lo que tenemos que hacer es dar de alta en la lista de las direcciones MAC su dirección. Recordamos que la dirección MAC es la del adaptador de red de cualquiera de los dispositivos que intente conectar con el router, ya sea PC o punto de acceso.

Lo normal es dar de alta las MAC de todos los equipos que queramos que accedan a la red inalámbrica. A partir de ese momento, el router no dejará acceder a la red inalámbrica a ningún dispositivo que no esté dado de alta en es tabla, evitando así las conexiones no deseadas en nuestra red, aunque tenemos dos posibilidades a configurar en la pantalla:

- Prevent (Evitar). Al hacer clic en este botón se bloqueará el acceso inalámbrico por dirección MAC.
- Permit Only (Permitir sólo). Al hacer clic en este botón se permitirá el acceso inalámbrico por dirección MAC.

Podemos pulsar el botón **Edit MAC Address Filter List** (Editar lista de filtros de direcciones MAC), que nos abrirá la lista de de filtros de direcciones MAC como vemos en la imagen

Imagen28

En esta pantalla se pueden enumerar por dirección MAC los usuarios a los que desea proporcionar o bloquear el acceso. Para facilitar la referencia, haga clic en el botón **Wireless Client MAC List** (Lista de MAC de clientes inalámbricos) para mostrar una lista de usuarios de la red por dirección MAC.

La última pestaña de configuración corresponde a **Advanced Wireless Settings** o *parámetros avanzados de configuración inalámbrica*, que vemos en la siguiente imagen:

Imagen29

Los parámetros a configurar son:

Authentication Type (Tipo de autenticación). El valor predeterminado está establecido en **Auto**, que permite utilizar la autenticación **Open System** (Sistema abierto) o **Shared Key** (Clave compartida).

Basic Rate (Velocidad básica). El parámetro **Basic Rate** corresponde a un conjunto de velocidades de transmisión a las que puede transmitir el router. El router comunica su velocidad básica a los demás dispositivos inalámbricos de la red para que conozcan las velocidades que se utilizarán y seleccionará automáticamente la mejor velocidad para la transmisión.

El parámetro predeterminado es **Default** (Predeterminado) cuando el router puede transmitir a todas las velocidades inalámbricas estándar (1-2 Mbps, 5,5 Mbps, 11 Mbps, 18 Mbps y 24 Mbps).

Si desea especificar la velocidad de transmisión de datos del router se debe configurar el parámetro Transmission Rate para indicar la velocidad de transmisión aunque lo adecuado es dejar los valores por defectos vistos anteriormente.

7.- Firewall

Si pinchamos sobre la pestaña **Security** accedemos a la configuración de parámetros de seguridad del router. La primera pantalla con la que nos encontramos es la de configuración del **Firewall** o *cortafuegos*, como vemos en la siguiente imagen:

Imagen30

Como podemos observar, existen varias *Check box* que nos permiten configurar las funciones del Firewall.
Tener activado el Firewall implica la inspección exhaustiva del tráfico de paquetes en nuestra red para ofrecer un control detallado de los paquetes de datos que entran en ella.

Las diferentes selecciones que se pueden usar son las siguientes:

- Block Anonymous Internet Requests:
Nos permite bloquear solicitudes anónimas de Internet evitando que otros usuarios de Internet sondeen o detecten la red. La función de bloqueo de solicitudes WAN también refuerza la seguridad de la red al ocultar los puertos de red. Esta función está activada de forma predeterminada. Si queremos permitir las solicitudes anónimas de Internet debemos desactivar la *check box*.

- Filter Multicast:
La multidifusión permite varias transmisiones simultáneas a receptores específicos. Si está seleccionada, el router permitirá que los paquetes Multicast IP se reenvíen a los ordenadores adecuados. Seleccionar para activar y filtrar las comunicaciones Multicast .

- Filter Internet NAT Redirection:
Esta función usa la opción de reenvío a puertos para bloquear el acceso a los servidores locales desde ordenadores en redes locales. Seleccionar para activar y filtrar la redirección NAT de Internet.

- Filter IDENT (Port 113):
Esta función impide que los dispositivos externos a la red local analicen el puerto **113**.
Seleccionar para activar y filtrar tráfico por el puerto 113.

Dentro de la pestaña **Security** hay una segunda opción y corresponde a **VPN Passthrough**, paso

a través de VPN (Virtual Private Network), que vemos en la siguiente imagen:

Imagen31

En esta pantalla tenemos la posibilidad de activar/desactivar mediante *Radio buttons* las opciones de filtrado por parte del Firewall de los protocolos IPSec, PPTP o L2TP en el tráfico a través de la VPN.

8.- Restricciones de acceso:

Disponemos también de funciones de restricción de acceso, a las que accederemos pulsando sobre la pestaña**Access Restrictions**, lo que nos presentará la siguiente pantalla:

Imagen32

La sección **Internet Access** permite bloquear o aceptar determinados tipos de uso y tráfico de Internet, como el acceso a Internet, servicios concretos, sitios Web y tráfico entrante a determinados días y horas. Este tipo de acciones se pueden configurar mediante la definición de las política de acceso y la creación de las diferentes reglas que sustentan esa política de acceso.

En la sección superior de este menú y pulsando el botón **Summary** accederemos a todas la reglas definidas, como vemos en la imagen:

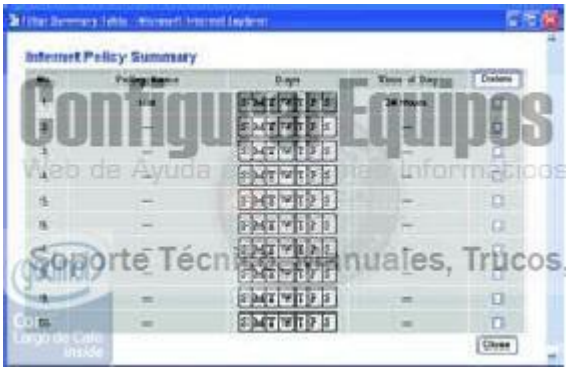


Imagen33

Estas reglas se pueden eliminar en la pantalla seleccionándolas y pulsando en el botón **Delete**.

Para volver a la ficha **Internet Access** (Acceso a Internet) haga clic en el botón **Close** (Cerrar).

Por defecto las reglas están desactivadas. Para activar una regla, debemos seleccionar su número en el menú desplegable (Imagen32) y hacer clic en el *botón de radio* **Enable**.

Las reglas que pueden ser creadas son de dos tipos, para administrar el acceso a Internet y para administrar el tráfico entrante.
Si queremos crear una regla de acceso a Internet, la operativa es la siguiente:

a.- Seleccionar un número en el menú desplegable **Internet Access Policy**.

b.- Para activar esta regla, seleccionamos en el *radio button* **Enable**.

c.- Damos un nombre a la regla en el campo **Enter Policy Name**.

d.- Seleccionamos **Internet Access en Policy Type** (Tipo de regla).

e.- Por último, pulsamos en el botón **Edit List** para seleccionar los PC a los que afectará esta

regla.

Al pulsar el botón aparecerá la pantalla como la que aparece en la siguiente imagen:

List of PCs
Enter MAC Address of the PCs in this format: xxxxxxxxxxxx
Enter the IP Address of the PCs
Enter the IP Range of the PCs
Save Settings
Cancel Changes

Imagen34

La selección de un PC se puede realizar por la dirección MAC de su adaptador de red o por la dirección IP asignada al adaptador. También es posible introducir un intervalo de direcciones IP si desea que la regla afecte a un grupo de PCs.

f.- Se seleccionará la opción que corresponda **Deny** o **Allow** (Imagen32) para denegar o permitir el acceso a Internet de los PC enumerados en la pantalla **List of PCs** (Lista de PC).

g.- Se puede indicar los días y las horas en que desea que se aplique esta regla, seleccionando cada día en que se aplicará la regla o **Everyday** si se quiere aplicar todos los días. Si se necesita, se puede indicar un intervalo de horas y minutos durante los que se aplicará la regla o 24 horas.

h.- Se puede filtrar el acceso a diferentes servicios a través de Internet, como FTP o Telnet, seleccionándolos en los menús desplegables que aparecen junto al texto **Blocked Services**, siendo posible bloquear hasta 20 servicios. Se podrá introducir también el intervalo de puertos que desea filtrar.
Si el servicio que queremos bloquear no se encuentra en la lista o es necesario editar los parámetros de un servicio, basta pulsar en el botón **Add/Edit Service** y aparecerá la pantalla **Port Services** que vemos en la imagen:

Imagen35

Si queremos agregar un servicio, se introduce el nombre en el parámetro **Service Name**, seleccionamos el protocolo usado por el servicio en cuestión en el menú desplegable **Protocol** y se introduce el intervalo en las cajas de texto **Port Range** pulsando en el botón **Add**.
Si deseamos borrar o modificar el servicio, se selecciona en la lista de derecha y se pulsa en el botón **Delete**o se modifican sus datos y se pulsa en el botón **Modify**. Para cerrar la pantalla y volver de nuevo a la pantalla**Access Restrictions** (Imagen32) pulsamos el botón **Close**.

i.- Si lo que queremos es bloquear sitios Web con direcciones URL concretas, se introducirá cada una en un campo independiente situado junto a **Website Blocking by URL Address**.

j.- Por último, si lo que queremos es bloquear sitios Web mediante palabras específicas, simplemente introducimos cada palabra en un campo situado junto a **Website Blocking by Keyword**.

En la imagen que ponemos a continuación se puede ver un ejemplo de estos dos últimos tipos de bloqueo:

Imagen36

Una vez introducidos los valores se debe hacer clic en el botón **Save Settings** para aplicar los cambios o en**Cancel Changes** para cancelarlos.

Si lo queremos crear una regla de control de tráfico entrante, la operativa es la siguiente:

a.- Seleccionamos en el desplegable **Policy Type** la opción **Inbound Traffic**, como vemos resaltado en la Imagen37

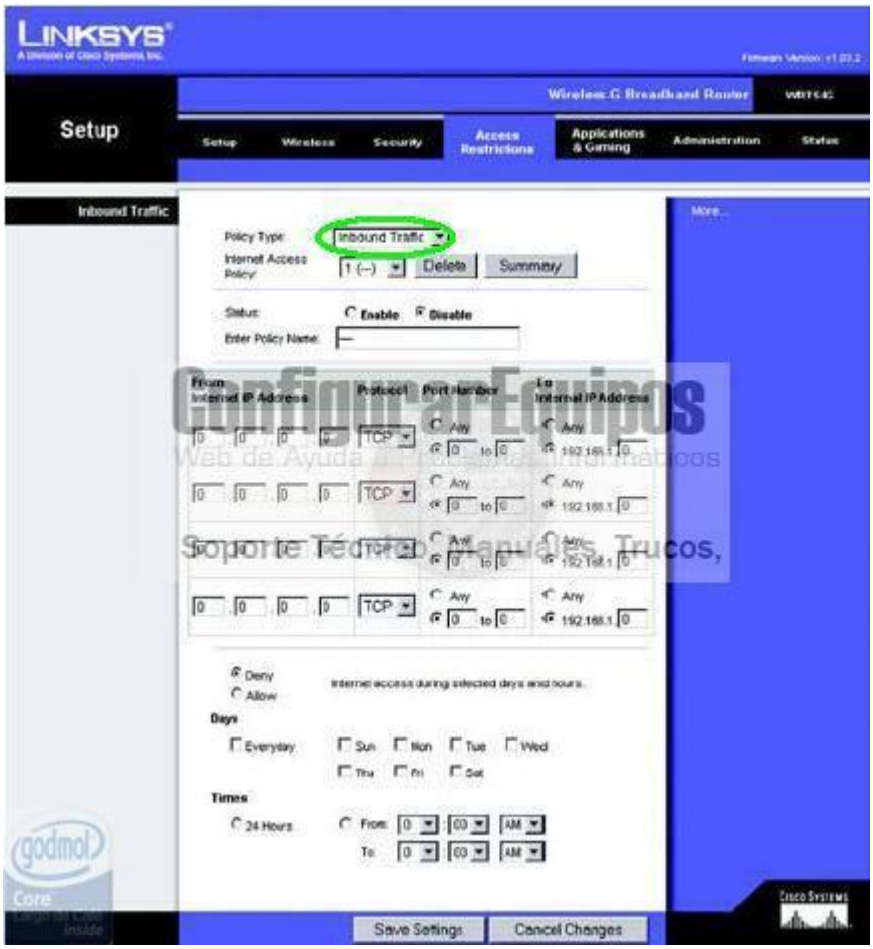



Imagen37

b.- Seleccionamos un número de regla en el menú desplegable **Internet Access Policy**.

c.- Para activar esta regla, seleccionamos el *radio button* para activar.

d.- Introducimos un nombre de regla en el campo **Enter Policy Name**.

e.- Se introduce la dirección IP de origen cuyo tráfico queremos administrar y se selecciona el protocolo correspondiente al tráfico a administrar que puede ser TCP, UDP o Both (Ambos), se

introducirá también el intervalo de puertos adecuado o **Any** para cualquier puerto y por último se introducirá la IP de destino cuyo tráfico queremos administrar.

f.- Seleccionamos el *radio button* de la opción deseada, **Deny** para denegar o **Allow** para Permitir.

g.- Se puede indicar los días y las horas en que desea que se aplique esta regla, seleccionando cada día en que se aplicará la regla o **Everyday** si se quiere aplicar todos los días. Si se necesita, se puede indicar un intervalo de horas y minutos durante los que se aplicará la regla o 24 horas.

Una vez introducidos los valores se debe hacer clic en el botón **Save Settings** para aplicar los cambios o en**Cancel Changes** para cancelarlos.

9.- Apertura de puertos:

Para acceder a esta sección de la configuración del router, es necesario acceder a la pestaña **Applications & Gaming**, que nos presentará la siguiente pantalla:

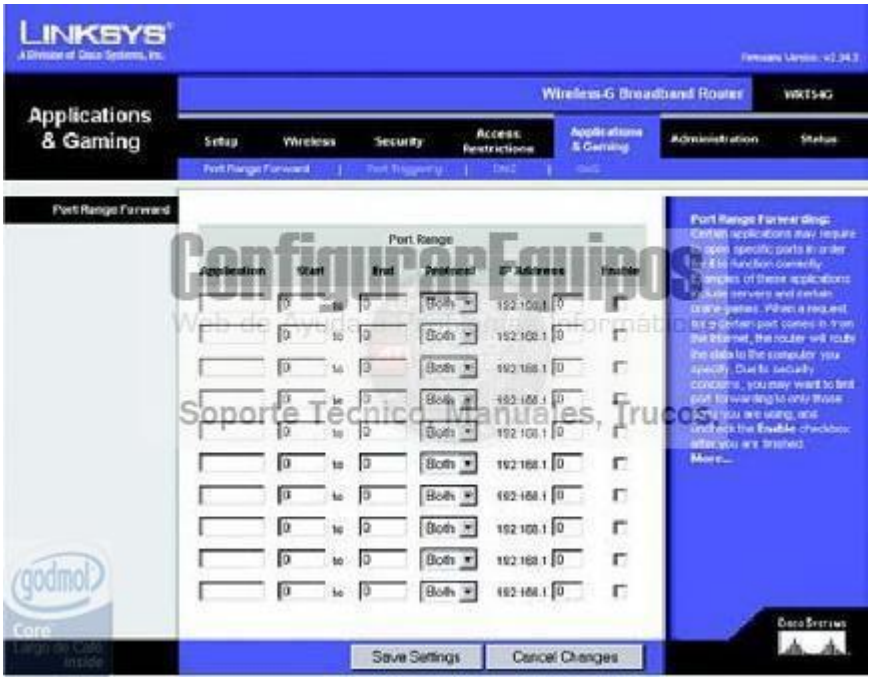


Imagen38

Y por defecto aparece la opción de configuración correspondiente a **Port Range Forward** o rango de envío de puertos que nos va a permitir configurar servicios públicos en la red, comoservidores Web, servidores FTP, servidores de correo electrónico u otras aplicaciones que utilizan el acceso a Internet para realizar funciones como videoconferencias o juegos en línea.

Introduciremos los datos en los parámetros para adaptarlos a las necesidades de redireccionamiento que queremos configurar estos datos son:

Application: Se debe introducir el nombre de hasta 12 caracteres que queremos asignar a la aplicación.
Start/End: Nos va a permitir introducir el intervalo de puertos, puerto inicial y final.
Protocol: Se debe especificar el protocolo usado por la aplicación en cuestión TCP, UDP o Both (Ambos).
IP Address: Se indicará la dirección IP interna del adaptador de red del ordenador que ejecuta la aplicación, por cada aplicación.
Enable: Seleccionaremos el *check box* **Enable** para activar el reenvío de puertos para la aplicación correspondiente.

Supongamos que estamos tratando de jugar en red a través del router y que nuestro juego usa el puerto**4678** y el protocolo **TCP**, y además el ordenador desde la que jugamos tiene la IP **192.168.1.35**. Podemos ver en la imagen inferior como se colocarían los datos:

Imagen39

También, dentro de la pestaña **Applications & Gaming**, podemos seleccionar la opción **Port Triggering**, con lo que nos aparecería esta pantalla:

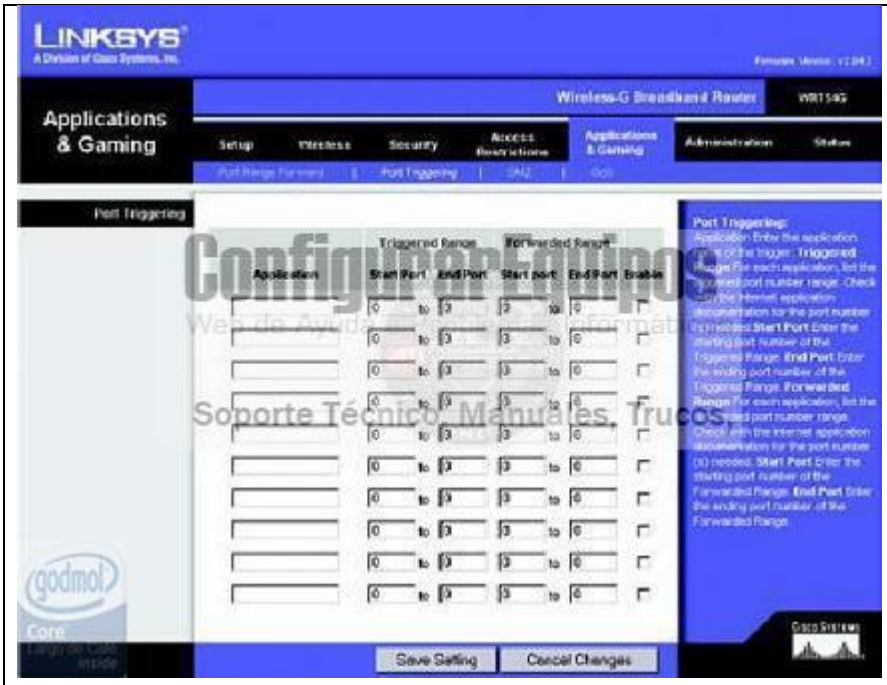


Imagen40

La pantalla **Port Triggering** permite realizar la configuración de algunas aplicaciones de manera que el router recuerda la dirección IP del ordenador que envía los datos coincidentes, de tal menera que, cuando los datos solicitados circulen a través del router, se dirijan al ordenador que corresponda mediante la dirección IP y las reglas de asignación de puertos.

Application: Se debe introducir el nombre de hasta 12 caracteres que queremos asignar a la aplicación
Triggered Range: Se debe introducir para cada aplicación el intervalo de números de puertos. Es necesario la consulta de la documentación de la aplicación de los números de puerto necesarios.
Start Port: Número de puerto inicial del intervalo desencadenado.
End Port: Número de puerto final del intervalo desencadenado.

Existen otras dos opciones más en la pestaña **Applications & Gaming**.
La primera es la función **DMZ**, que permite exponer a un usuario de red a Internet para el uso de un servicio especial, como juegos por Internet y video conferencias sin pasar por las medidas de seguridad establecidas por las opciones definidas en el apartado **Security**.
La segunda es **QoS**. La configuración del servicio **QoS** permite garantizar un mejor servicio para tipos de tráfico de red de alta prioridad. Suele usarse para trabajar con aplicaciones en tiempo real y muy exigentes, como las video conferencias.

10.- Administración y Estado:

Dentro del configurador web del router, nos falta por explicar el significado de las dos últimas pestañas y es lo que vamos a describir en este ultimo punto del tutorial.

Administración:

La pestaña en cuestión nos va a permitir configurar en el router una serie de funciones específicas relacionadas con su funcionamiento. Existen varios botones pero al pulsar sobre la pestaña nos aparece por defecto la pantalla que vemos a continuación.

Imagen41

Aparece seleccionada la opción de **Menú Management** en el que podremos configurar algunas funciones específicas del router, como puede ser el cambio de contraseña en la sección **Local Router Access**. Basta con introducir la nueva contraseña en el campo **Router password** y, a continuación, volver a escribirla en el campo **Re-enter to confirm** para confirmarla.

En la sección **Web Access** se establece el protocolo de acceso Web a servidores a través de HTTP o si se desea aumentar la seguridad HTTPS que usa SSL para encriptar las comunicaciones.

Wireless Access Web para habilitar o deshabilitar el acceso inalámbrico a la utilidad de configuración Web.

La sección **Remote Router Access** nos sirve para acceder al router de forma remota, desde fuera de la red, en cuyo caso ha de esta marcada la opción **Enable**. Podemos definir además un puerto a través del cual comunicar con el exterior, y habrá que indicárselo.

La sección **UPnP** permite activar el uso de las funciones UPnP en el router.

La siguiente opción de menú en la pestaña Administration es **Log**, como vemos en la siguiente imagen:

Imagen42

La función **Log** activada permite almacenar los datos de las conexiones entrantes o salientes pulsando los botones **Incoming Log** u **Outgoing Log**.

Otra funcion configurable en la pestaña Administration es **Diagnostics**, como vemos en la siguiente imagen:

Imagen43

En esta pantalla se nos permite realizar algunas pruebas de diagnóstico de funcionamiento de nuestro router,**Ping Test**, que comprueba el estado de una conexión y **Traceroute Test** para probar el rendimiento de una conexión con un determinado PC.

Para finalizar veremos las tres últimas opciones de esta pestaña Administration y que

corresponden a **Factory Defaults**, que nos permite restablecer los parámetros de configuración de fábrica:

Imagen44

Firmware Upgrade, que nos permite actualizar el firmware del router pulsando en el botón **Upgrade** e indicando la ubicación del fichero de actualición como podemos ver en la imagen:

Imagen45

La última función es **Config Management**, que se utiliza para realizar una copia de seguridad del archivo de configuración del router o para restaurar la copia

Imagen46

Si queremos hacer una copia de seguridad del archivo de configuración del router, basta con pulsar el botón**Backup** y seguir las instrucciones que aparecen en la pantalla.

Si lo que queremos es restaurar el archivo de configuración del router, pulsamos el botón **Browse** para localizarlo y seguir las instrucciones que aparecen en la pantalla. Una vez seleccionado el archivo, pulsamos el botón **Restore**.

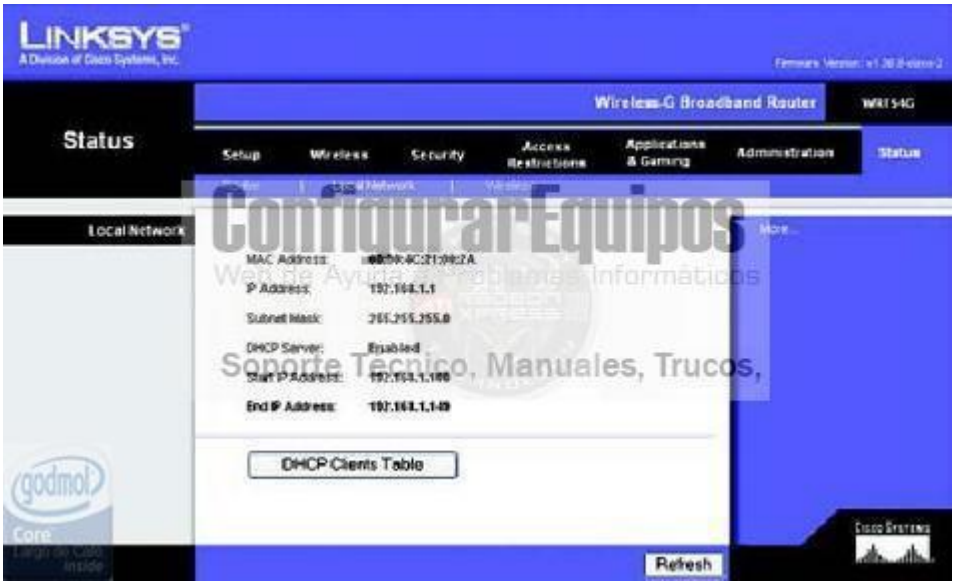
Estado:

La última pestaña por describir es la correspondiente a **Status**, en la que hay varias opciones:

Ver el estado del router:

La información que se visualiza es la Versión del firmware, la Hora actual, la Dirección MAC, el Nombre del router y el Nombre de host y Nombre de dominio si fueron introducidos

ver el estado de la red local:



Donde se visualizan los datos relativos a la Dirección MAC del router tal como se ve en la red local, la Dirección IP, la Máscara de subred, si está o no habilitado el Servidor DHCP, las Dirección IP inicial y final del intervalo de direcciones IP que utilizan los dispositivos de la red local.

Desde esta misma pantalla podemos visualizar la lista de los clientes DHCP a los que el router ha proporcionado las IP de manera dinámica como se ve en la siguiente imagen:

Ver el estado de la red inalámbrica:

Por último podemos consultar **Ver el estado de la red inalámbrica**, visualizando la dirección MAC del router tal como se ve en la red inalámbrica, el modo inalámbrico usado, el nombre de red inalámbrica o SSID, el canal en el que emite la red inalámbrica, si existe encriptación y el tipo de encriptación tal como se haya seleccionado en la pestaña Security.

ACTIVIDAD 1 DE INALAMBRICAS

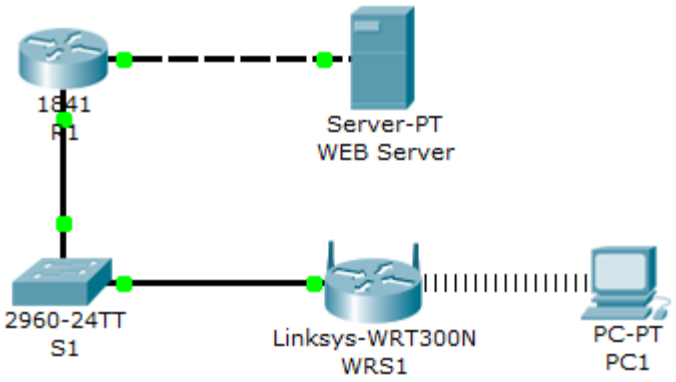
Descripción de la actividad: El estudiante maneja los Conceptos básicos y características fundamentales diseño e implementación de redes de comunicaciones wi-fi e hibridas; el estudiante revisa material de video y escrito expuesto por el instructor, consulta textos y videos sobre redes de cómputo para la configuración de redes inalámbricas.

Realiza el siguiente taller de configuración de AP y Gestión básica de red basado en la exposición docente y las consultas de documentación para configuración de equipos inalámbricos

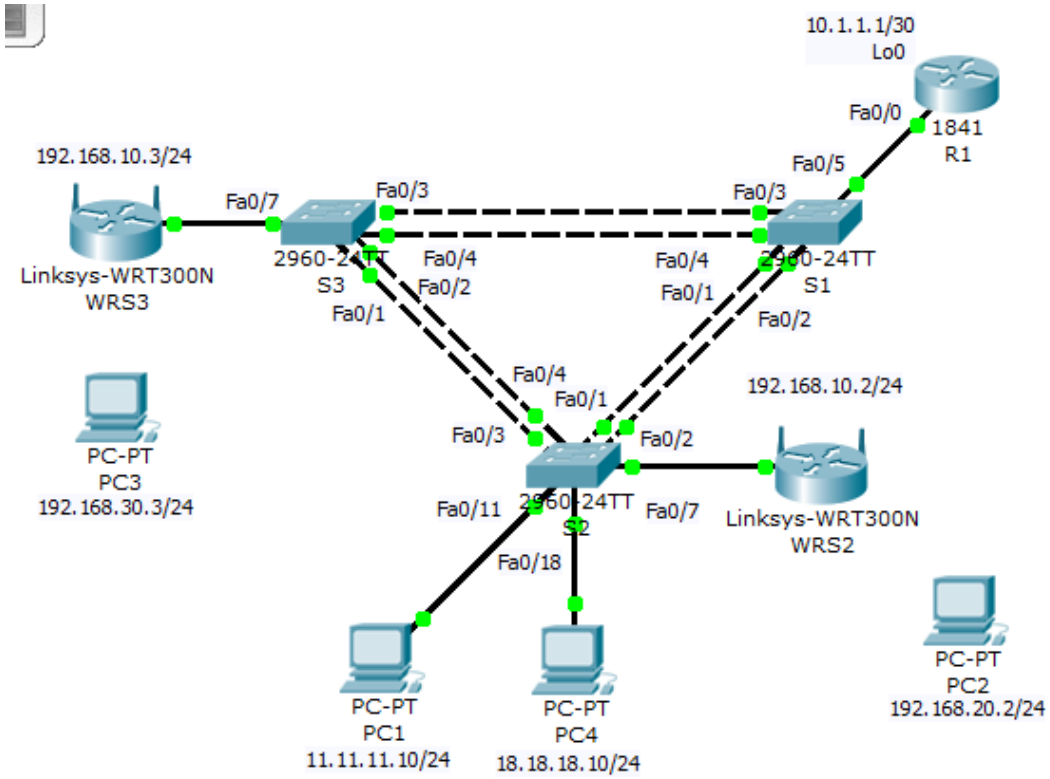
Laboratorio 1 Sesión 1

Realiza en el simulador Cisco Packet Tracer el siguiente esquema

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	Fa0/1	10.10.50.1	255.255.255.0	N/A
	Fa0/1	10.10.1.1	255.255.255.0	N/A
WRS1	WAN	10.10.1.2	255.255.255.0	10.10.1.1
	LAN/Wireless	10.10.10.1	255.255.255.0	N/A
PC1	NIC	DHCP Assigned	DHCP Assigned	DHCP Assigned
WEB Server	NIC	10.10.50.254	255.255.255.0	10.10.50.1



Laboratorio 2 Sesión 1



Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	Fa0/0.5	5.5.5.10	255.255.255.0	N/A
	Fa0/0.10	192.168.10.1	255.255.255.0	N/A
	Fa0/0.11	11.11.11.1	255.255.255.0	N/A
	Fa0/0.18	18.18.18.1	255.255.255.0	N/A
	Lo0	10.1.1.1	255.255.255.252	N/A
WRS2	WAN	192.168.10.2	255.255.255.0	192.168.10.1
	LAN/Wireless	192.168.20.1	255.255.255.0	N/A
WRS3	WAN	192.168.10.3	255.255.255.0	192.168.10.1
	LAN/Wireless	192.168.30.1	255.255.255.0	N/A
PC1	NIC	11.11.11.10	255.255.255.0	11.11.11.1
PC4	NIC	18.18.18.10	255.255.255.0	18.18.18.1
S1	VLAN 5	5.5.5.1	255.255.255.0	N/A
S2	VLAN 5	5.5.5.2	255.255.255.0	N/A
S3	VLAN 5	5.5.5.3	255.255.255.0	N/A

ACTIVIDAD 2 DE INALAMBRICAS

1. Conforme un equipo de trabajo de 4 personas y verifique que cuenta con el material necesario para la práctica, esto es:
    a. 1 Punto de Acceso (AP)
    b. 2 equipos con tarjetas inalámbricas (PC con Tarjeta Inalámbricas)

    Nota: Verifique que las tarjetas inalámbricas sean compatibles con el Punto de Acceso.

2. Consulte la información técnica de los dispositivos y realice un resumen de sus principales características.

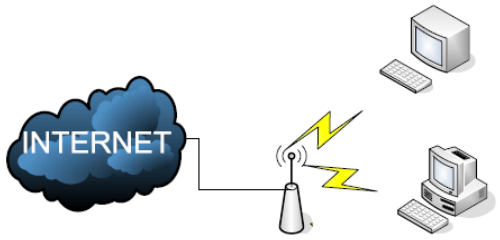
3. Instale y configure el Punto de Acceso teniendo en cuenta las siguientes recomendaciones:
    a. Conecte su equipo al Punto de Acceso. ¿Qué tipo de cable debe utilizar? Muestre en evidencias lo realizado
    b. Ingrese al modo de configuración o administración del Punto de Acceso. ¿Qué consideraciones debe tener en cuenta?
    c. Realice la configuración básica del Punto de Acceso. Esto es: Nombre de la WLAN (SSID); Canal, Modo de Operación y direccionamiento lógico (Dirección IP y Máscara de Subred). Para este caso utilice una subred diferente a la que se encuentra en la Sala de Redes.
    d. ¿Cómo puede determinar si la WLAN está funcionando?
    e. ¿Qué otros parámetros de configuración tiene el Punto de Acceso? Indague su utilidad.

4. Instale y configure las Tarjetas Cliente WLAN según las siguientes especificaciones:
    a. De acuerdo al tipo de Tarjeta WLAN realice su conexión física.
    b. Instale el driver de la Tarjeta WLAN. ¿Observa algún cambio en su Sistema Operativo?
    c. Configure su Tarjeta WLAN para que pueda conectarse con el Punto de Acceso configurado en el paso anterior. ¿Qué consideraciones debe tener en cuenta para realizar esta conexión?
    d. Utilizando la herramienta de Windows para conexiones inalámbricas o la herramienta software propietario de la tarjeta WLAN, determine que WLANs detecta su tarjeta WLAN. ¿Qué información adicional suministra la herramienta?
    e. Conéctese a la WLAN creada en el paso anterior. ¿Con qué comando pueden determinar si realmente están conectados? Realice la prueba.
    f. Realice pruebas de conexión y transferencia de archivos entre los equipos inalámbricos configurados (Tarjeta WLAN1 <-> Tarjeta WLAN2)

5. En los equipos que contienen las Tarjetas Cliente WLAN instale el Software **Inssider**, y ejecútelo. ¿Qué utilidades posee la herramienta?; ¿Qué datos está visualizando?; ¿Existe alguna otra WLAN configurada en el mismo canal?

6. Instale y configure una Red AdHoc inalámbrica entre dos equipos. Para esto utilice el utilitario de Windows en <<Ver redes inalámbricas disponibles>>.
    a. ¿Qué opciones diferentes observa entre la configuración de una red tipo infraestructura y una red tipo AdHoc?
    b. Realice pruebas de conexión entre los equipos inalámbricos configurados (Tarjeta WLAN1 <-> Tarjeta WLAN2)

7. Instale y configure el siguiente esquema de Red Inalámbrica. Garantice que los clientes tengan acceso a Internet.



Nota: Si el Punto de Acceso asignado soporta DHCP configúrelo de tal forma que le sea asignado a los clientes direcciones dinámicas, de lo contrario configure direcciones estáticas.

ACTIVIDAD 3 DE INALAMBRICAS

1. Realice las siguientes pruebas de transmisión de datos.

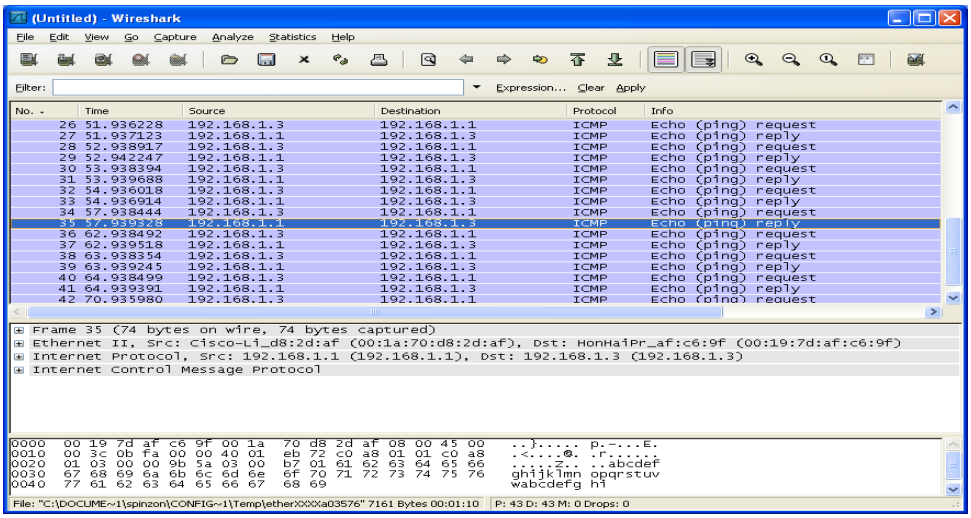
a. Instale un servidor FTP en uno de los equipos con Tarjeta WLAN y realice transferencia de archivos de diferentes tamaños (500K, 1M, 5M, 10M, 100M) entre los equipos con Tarjeta Inalámbrica. Realice una tabla y grafique indicando tamaño del archivo vs. Tasa de transferencia y Tiempo de la transferencia. ¿Qué observa al respecto? Tome nota de los valores de RSSI de las Tarjetas WLAN.

b. Apague el Punto de Acceso y ubíquelo en un sitio tal que el valor de RSSI de por lo menos una de las Tarjetas WLAN esté por debajo de los -80 dBm. Realice la misma prueba del punto a. Realice una tabla y grafique indicando tamaño del archivo vs. Tasa de transferencia y Tiempo de la transferencia. ¿Qué observa al respecto? Tome nota de los valores de RSSI de las Tarjetas WLAN.

c. Desconecte las tarjetas inalámbricas de los equipos y realice la misma prueba anterior empleando la red cableada. Realice una tabla y grafique indicando tamaño del archivo vs. Tasa de transferencia y Tiempo de la transferencia. ¿Qué observa al respecto?

d. ¿Qué diferencias observa entre el punto a y c?

2. Instale el software WireShark. Este le permitirá realizar capturas de paquetes 802.11. ¿Qué puede observar de las tramas 802.11?, ¿Es fácil detectar las direcciones MAC de los equipos clientes que están conectados? Para iniciar la captura: Capture >> Interfaces >> Seleccione la Tarjeta WLAN correspondiente >> Start


(Untitled) - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter: Expression... Clear Apply
No. - Time Source Destination Protocol Info
26 51.936228 192.168.1.3 192.168.1.1 ICMP Echo (ping) request
27 51.937123 192.168.1.1 192.168.1.3 ICMP Echo (ping) reply
28 52.938917 192.168.1.3 192.168.1.1 ICMP Echo (ping) request
29 52.942247 192.168.1.1 192.168.1.3 ICMP Echo (ping) reply
30 53.938394 192.168.1.3 192.168.1.1 ICMP Echo (ping) request
31 53.939688 192.168.1.1 192.168.1.3 ICMP Echo (ping) reply
32 54.936018 192.168.1.3 192.168.1.1 ICMP Echo (ping) request
33 54.936914 192.168.1.1 192.168.1.3 ICMP Echo (ping) reply
34 57.938444 192.168.1.3 192.168.1.1 ICMP Echo (ping) request
35 57.939343 192.168.1.1 192.168.1.3 ICMP Echo (ping) reply
36 62.938492 192.168.1.3 192.168.1.1 ICMP Echo (ping) request
37 62.939518 192.168.1.1 192.168.1.3 ICMP Echo (ping) reply
38 63.938354 192.168.1.3 192.168.1.1 ICMP Echo (ping) request
39 63.939245 192.168.1.1 192.168.1.3 ICMP Echo (ping) reply
40 64.938499 192.168.1.3 192.168.1.1 ICMP Echo (ping) request
41 64.939391 192.168.1.1 192.168.1.3 ICMP Echo (ping) reply
42 70.935980 192.168.1.3 192.168.1.1 ICMP Echo (ping) request
Frame 35 (74 bytes on wire, 74 bytes captured)
Ethernet II, Src: Cisco-Li_d8:2d:af (00:1a:70:d8:2d:af), Dst: HonHaiPr_af:c6:9f (00:19:7d:af:c6:9f)
Internet Protocol, Src: 192.168.1.1 (192.168.1.1), Dst: 192.168.1.3 (192.168.1.3)
Internet Control Message Protocol
0000 00 19 7d af c6 9f 00 1a 70 d8 2d af 08 00 45 00 ..}..... p.-...E.
0010 00 3c 0b fa 00 00 40 01 eb 72 c0 a8 01 01 c0 a8 .<....@. .r......
0020 01 03 00 00 9b 5a 03 00 b7 01 61 62 63 64 65 66 .....Z.. ..abcdef
0030 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 ghijklmn opqrstuv
0040 77 61 62 63 64 65 66 67 68 69 wabcdefg hi
File: "C:\DOCUME~1\spinzon\CONFIG~1\Temp\etherXXXXa03576" 7161 Bytes 00:01:10
P: 43 D: 43 M: 0 Drops: 0

3. Verifique la clave de conexión de un cliente al servidor FTP desde una terminal donde tenga corriendo el wireshark

Nota: La evidencia es el documento dando respuesta a la preguntas y donde muestre la realización de la práctica y pruebas correspondientes; debe ser enviada a profearias9@hotmail.com con el asunto (actividad cisco UTS)